CCNA Study Guide

Alexander

June 9, 2024

1. Network Fundamentals (20%)
2. Network Access (20%)
3. IP Connectivity (25%)
4. IP Services (10%)
5. Security Fundamentals (15%)
6. Automation and Programmability (10%)

Network Fundamentals

- Explain the role and function of network components

  Routers forward packets between computer networks (LANs and WANs), and use IP addresses to determine where a packet should go. Routers remove data-link headers and trailers, analyze packet information, and then re-encapsulate the data with a new data-link frame before transmission. Routers compare destination IPs, found inside packet headers, to routes in routing tables before forwarding packets. Routing tables get their routes from static routes, dynamic routing protocols, and source headers fields found in packets recieved on local interfaces. Routers can perform many different actions: implementing QoS tools, permiting/denying packets with ACLs, performing firewall functions, advertising BSSs, and more.

  L2 switches forward data frames within the same network segment using MAC addresses found in data-link frames. Switches learn MAC addresses from the source fields located in the frame and place this information in a table. Switches divide collision domains; unlike routers, which divide broadcast domains. L3 switches can perform both switching and routing functions.

  Firewalls sit in the path that packets take through the network. They permit/deny traffic much like an ACL would do on a router. Firewalls are capable of watching application-layer flows with AVC, performing webpage verification on URIs, and retaining state. IPSs can compare packet flows to exploit signatures, log events, and can discard/redirct packets.

  An AP serves as a single point of contact for every device that wants to use a BSS. An AP uses a unique BSSID that is based on the AP's own radio MAC address. APs are often connected to a DS that uplinks to a wired network.

- Describe characteristics of network topology architectures
- Compare physical interface and cabling types
- Identify interface and cable issues (collisions, error, mismatch duplex, and/or speed)
- Compare TCP to UDP
- Configure and verify IPv4 addressing and subnetting

  ```
  Router(config-if)# ip address <ip_address> <subnet_mask>

  Router# show ip interface brief
  ```

- Describe private IPv4 addressing
- Configure and verify IPv6 address types

  ```
  Router(config-if)# ipv6 address <IPv6_address>/<prefix_length>

  Router# show ipv6 interface brief
  ```

- Describe IPv6 addressing and prefix
- Verify IP parameters for Client OS
- Describe wireless principles
- Explain virtualization fundamentals (server virtualization, containers, and VRFs)
- Describe switching concepts

Network Access

- Configure and verify VLANs (normal range 0-1005) spanning multiple switches

  1. create vlan, 2. port operational mode, 3. apply port

  ```
  Switch(config)# vlan <vlan-id>
  Switch(config-if)# switchport mode access
  Switch(config-if)# switchport access vlan <vlan-id>
  ```

troubleshoot: VLANs defined/active, configuration mismatches, VTP, DTP, operational mode

```
Switch# show vlan [brief]
Switch# show interface interface_type interface_number [brief]
Switch# show interfaces status
Switch# show run
```

- Configure and verify interswitch connectivity

  1. operational mode, 2. allowed vlans, 3. trunking standard, 4. native vlan

  ```
  Switch(config-if)# switchport mode trunk
  Switch(config-if)# switchport trunk allowed vlan <10,20,30>
  Switch(config-if)# switchport tunk encapsulation <dot1q/isl>
  Switch(config-if)# switchport trunk native vlan <vlan-id>
  ```

  troubleshoot: VLANs defined/active, configuration mismatches, VTP, DTP, operational mode

  ```
  Switch# show interface trunk
  Switch# show interfaces switchport
  Switch# show interface interface_name interface_number
  ```

- Configure and verify L2 discovery protocols (CDP/LLDP)

  CDP: device IDs, addresses, ports, capabilities, platform, etc.

  ```
  Switch(config-if)# cdp enable (enable cdp on an interface)
  Switch(config)# cdp run (how to manually enable it gloablly)
  Switch# show cdp neighbors <interface_type><interface_number>(one summary line about the neighbor)
  Switch# show cdp neighbors detail (lists one large set of information)
  Switch# show cdp entry name (similar to the command above, but only for the named neighbor)
  Switch# show cdp interface <interface_type ><interface_number>(is cdp enabled, cdp timers)
  Switch# show cdp (is cdp enabled, timer details)
  Switch# show cdp traffic (advertisment stats)
  ```

  LLDP: Cisco devices globally enable CDP by default and disable LLDP

  ```
  Switch(config)# lldp run
  Switch(config-if)# lldp transmit
  Switch(config-if)# lldp receive
  ```

- Configure and verify (L2/L3) EtherChannel (LACP)

  Manual Configuration:

  ```
  Switch(config-if-range)# channel-group 1 mode on Switch(config)# port-channel load-balance method (src. and or dest. MACs/IPs/port numbers)
  ```

Dynamic Congifuration:
Switch(config-if-range)# channel-group 1 mode <desirable/auto>(PAgP)
Switch(config-if-range)# channel-group 1 mode <active/passive>(LACP)

troubleshoot: speed, duplex, operational mode, VLANs, Spanning Trees
Switch# show etherchannel summary
Switch# show interfaces status

L3 Etherchannel configuration is similar to L2 configuration however:
1. each physical port needs to be a routed port (no switchport command)
2. the actually channel needs to be a routed port with an IP and mask

- Interpret basic operations of Rapid PVST+ Spanning Tree Protocol
- Describe Cisco Wireless Architectures and AP modes
- Describe physical infrastructure connections of WLAN components (AP, WLC, access/trunk ports, and LAG)
- Describe network device management access (Telnet, SSH, HTTP, HTTPS, console, TACACS+/RADIUS, and cloud managed)
- Interpret the wireless LAN GUI configuration for client connectivity, such as WLAN creation, security settings, QoS profiles, and advanced settings

IP Connectivity

- Interpret the compnents of routing table
- Determine how a router makes a forwarding decision by default
- Configure and verify IPv4 and IPv6 static routing

  Default routes are used when a packet's destination address does not match any routes, but you do not want the router to discard a packet that it otherwise would.
  Router(config)# ip route 0.0.0.0 0.0.0.0 interface_name interface_number

  Network routes define a route to an entire subnet.
  Router(config)# ip route 172.16.2.0 255.255.255.0 s0/0/0
  Router(config)# ip route 172.16.3.0 255.255.255.0 172.16.5.3

  Host routes match a single IP. An engineer may want to route most packets to some subnet through one route but packets destined for a specific host through another route.
  Router(config)# ip route 10.1.1.9 255.255.255.255 10.9.9.9

  Floating static routes are used when when a primary route fails.

  ```
  Router(config)# ip route 172.16.2.0 255.255.255.0 172.16.5.3 130
  ```

- Configure and verify single area OSPFv2

  OSPF Configuration Mode:

  ```
  Router(config)# router ospf <1-65535>
  Router(config-router)# router-id 1.1.1.1 (OPTIONAL)
  Router(config-router)# network <ip_address><network_mask>
  ```

  Indirect Configuration Through Interface Mode:

  ```
  Router(config-if)# ip address 10.1.1.1 255.255.255.0
  Router(config-if)# ip ospf 1 area 0
  ```

  Show commands:

- Describe the purpose, functions, and concepts of first hop redundancy protocols

IP Services

- Configure and verify inside source NAT using static and pools
- Configure and verify NTP operating in a client and server mode
- Explain the role of DHCP and DNS within the network
- Explain the function of SNMP in network operations
- Describe the use of syslog features including facilities and levels
- Configure and verify DHCP client and relay
- Explain the forwarding per-hop behavior (PHB) for QoS, such as classification, marking, queuing, congestion, policing, and shaping
- Configure network devices for remote access using SSH
- Describe the capabilities and functions of TFTP/FTP in the network

Security Fundamentals

- Define key security concepts (threats, vulnerabilities, exploits, and mitigation techniques)
- Describe security program elements (user awareness, training, and physical access control)
- Configure and verify device access control using local passwords

- Describe security password policies elements, such as management, complexity, and password alternatives (multifactor authentication, certificates, and biometrics)
- Describe IPsec remote access and site-to-site VPNs
- Configure and verify access control lists
- Configure and verify Layer 2 security features (DHCP snooping, dynamic ARP inspection, and port security)
- Compare authentication, authorization, and accounting concepts
- Describe wireless security protocols (WPA, WPA2, and WPA3)
- Configure and verify WLAN within the GUI using WPA2 PSK

Automation and Programmability

- Explain how automation impacts network management
- Compare traditional networks with controller-based networking
- Describe controller-based, software defined architecture (overlay, underlay, and fabric)
- Explain AI (generative and predictive) and machine learning in network operations
- Describe characteristics of REST-based APIs (authentication types, CRUD, HTTP verbs, and data encoding)
- Recognize the capabilities of configuration management mechanisms, such as Ansible and Terraform
- Recognize components of JSON-encoded data